FORTINET
High Performance Network Security

FortiWLM

Release 8.3.2
(Virtual Controllers)

Fortinet Wireless LAN Virtual Controllers

FortiWLM 8.3.2 is a **limited release delivering the new Virtual Controllers**, **FWC-VM-50, FWC-VM-200, FWC-VM-500, FWC-VM-1000**, and **FWC-VM-3000**. FortiWLM supports the above virtual controller models created in VMware ESXi, Hyper-V and KVM virtualization infrastructures.

Additionally, this release also introduces features and enhancements as listed under the New Features section.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Getting Started with Upgrade

This section describes procedures for upgrading your Services Appliance.

Pre-requisites for Upgrade

Upgrade service appliances (SA / FWLM) before you initiate controller (FortiWLC-SD) upgrade.
While upgrading a Services Appliance with over 100 controllers, the controllers return to *active* state sequentially, one at a time. It may take up to 10 minutes or more for all controllers to become active.

Supported FortiWLM Upgrades

The following upgrade path is recommended.

From FortiWLM version…	To FortiWLM version
6.1-3-6/7.0-5-0	8.0-7-0
6.1-3-6/7.0-5-0/8.0-7-0	8.0-SR1-1
8.0-7-0/8.0-SR1-1	8.1-2-0
7.0-5-0/8.0-7-0/8.1-2-0	8.2-2-0
8.1-2-0/8.2-2-0	8.2-4-0 (MR)
8.1-2-0/8.2-2-0	8.3-0-6
8.2-4-0/8.3-0-6	8.3-1-1 (MR)
8.2-4-0/8.3-0-6/8.3-1-1	8.3-2-1

Supported FortiWLC-SD Releases

Network Manager Version	Supports Controllers with these FortiWLC-SD Versions
8.3.2	• 7.0-9-1 • 7.0-10-MR • 8.0-6-0-MR • 8.1-2-0 • 8.1-3-2MR • 8.2-4-0 • 8.2-7 • 8.3.0 • 8.3.1 • 8.3.2

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
FortiWLM/SAM - Access Points	• AP110 • AP122 • AP320 • AP332 • AP433 • OAP433 • AP822 • AP832 • AP1020 • AP1014 • OAP832 • FAP-U421EV • FAP-U423EV

Hardware / Software	Supported Versions/Models
SM	• AP332 • AP832 • PSM3x • AP1010 • AP1020 • FAP-U421EV • FAP-U423EV
Controller Models	• FortiWLC-200D • FortiWLC-500D • FortiWLC-50D • FortiWLC-1000D • FortiWLC-3000D • MC1550 • MC1550-VE • MC3200 • MC3200-VE • MC4200 • MC4200-VE • FWC-VM-50 • FWC-VM-200 • FWC-VM-500 • FWC-VM-1000 • FWC-VM-3000
Service Appliance	• FortiWLM-100D • FortiWLM-1000D • SA250 • SA2000 • SA2000-VE • FWM-VM • Hyper-V • KVM
	# Due to hardware limitations, High Availability is not supported in FortiWLM100D and SA250 appliances.

Supported Browsers	• Internet Explorer 9 and later version *All the pages of EzRF will load under normal browser settings. Compatibility View Settings are not supported.* • Mozilla Firefox 32.0 • Google Chrome, version 34.0.1847.118 m

Application Visibility Policies

Application visibility policies in controllers running FortiWLC-SD 8.0 that is managed by FortiWLM 8.1 or later will be disabled. To continue using those policies, upgrade FortiWLC-SD to 8.1 or later.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

When upgrading from versions prior to FortiWLM 7.0, the DB is reset. It is therefore recommended that database backup should be taken before upgrade and restored after upgrade.

Upgrading via CLI

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
    a. Select **Service Assurance**.
    b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
    c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

    ```
    sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
    ```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

    ```
    sa# sh flash
    6.0-7-0 8.2-
    1-0
    ```

7. Upgrade the service appliance:

    ```
    sa# upgrade nms-server <Version>
    ```

    This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes and at the end of the upgrade the services appliance restarts. The time taken to upgrade, depends on the size of the data available on the services appliance.
8. Type the following command to confirm, if the installed software version is 8.3.2.

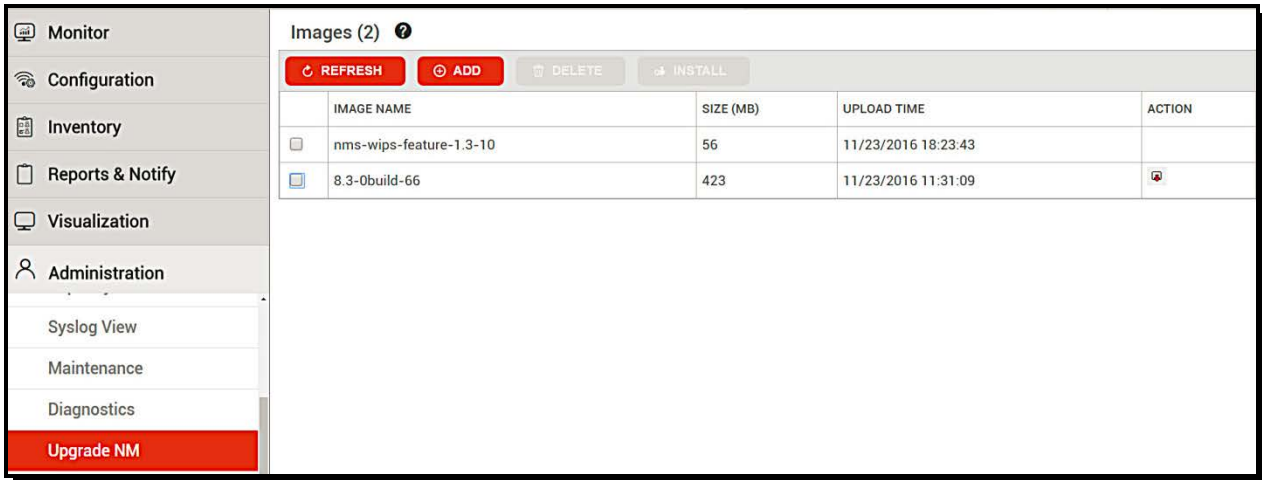
    ```
    service appliance# sh nms
    ```

If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

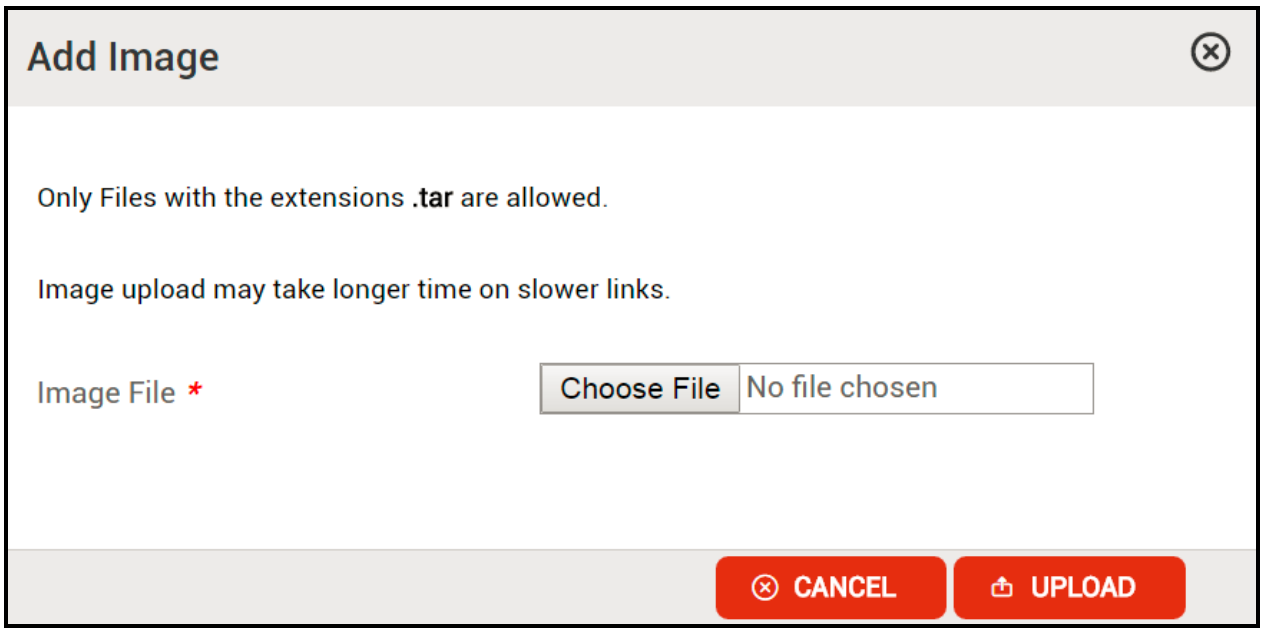
Upgrading via WebUI

The following procedure will guide you through the steps to upgrade your server from WebUI.

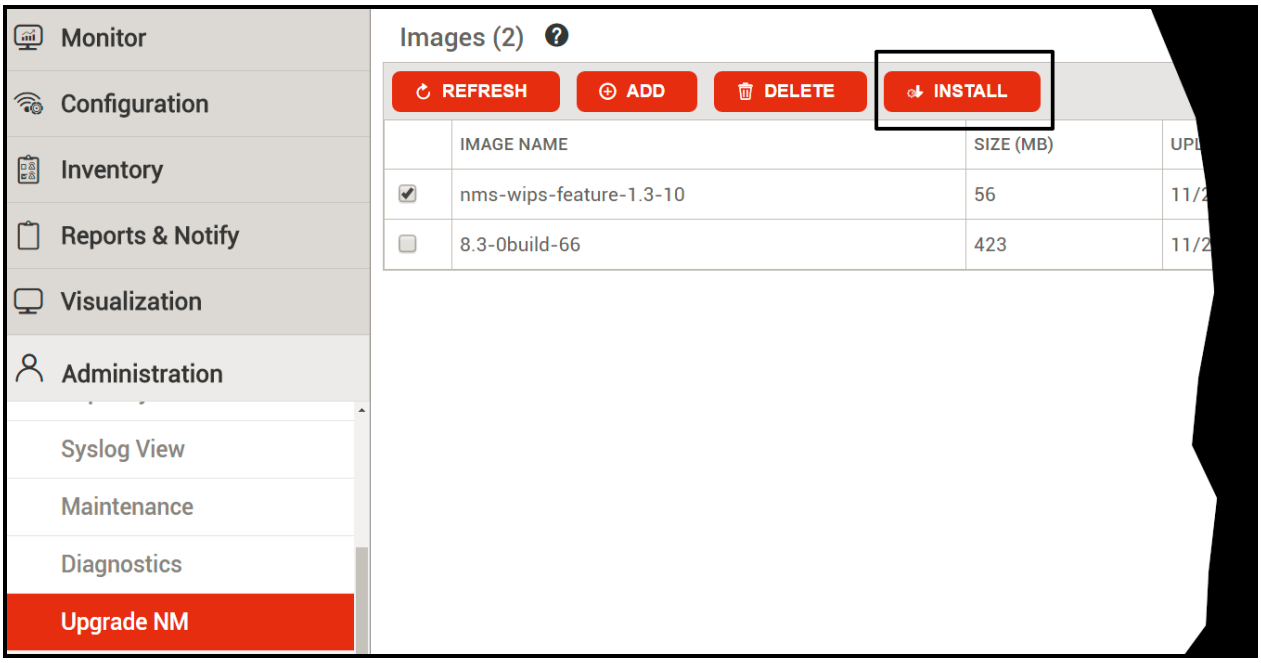
1. In the Network Manager WebUI, go to Administration > System Administration > Upgrade NM. By default, this page lists all the images copied to the server.



2. To upgrade your server to a different version than the ones listed, click **Add** to open the file selector window.



3. Select the image file from your computer or a network folder and click the **UPLOAD** button
4. After the upload is complete, select the version to install and click the **INSTALL** button to being the upgrade process.



During the upgrade process, do not click refresh or perform any operations on the server.

After the upgrade is complete, click Go the link to return to server operations.

- For a full upgrade, the server will restart after the upgrade process and return the page to server login prompt.
- For patch upgrade, the server will restart the process and return to the dashboard.

Post Upgrade Tasks

The following are optional post-upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration** > **Maintenance** page.
2. If required, upload the license.

Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

Downgrade

Downgrading FortiWLM to a previous version is not supported. To go back to an older version of FortiWLM, you must do a fresh install of that version on your FortiWLM server.

Deploying FWLM VM on VMWare ESXi

This document describes the procedure to deploy FWLM-VM-100D and FWLM-VM-1000D on VMWare ESXi.

Note: Fortinet recommends VMWare ESXi version 6.5.

Supported Hardware Configuration

This table lists the supported configuration for FWLM-VM-100D and FWLM-VM-1000D.

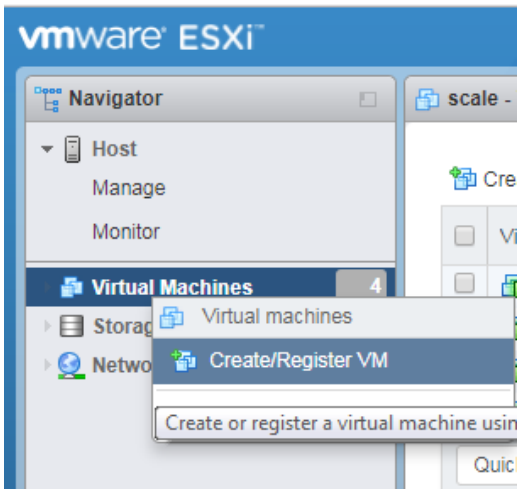
Configuration	FWLM-VM-100D	FWLM-VM-1000 D
Processor and Cores	Any Processor @ 2GHz or Higher. 4 Cores - 4 Threads	Any Processor @ 3.20GHz or Higher. 4 Cores - 8 Threads
Memory (DRAM)	4GB	16GB
Storage	1TB	2TB
Minimum Disk I/O	100MBps	100MBps
Network	1-4 1G RJ-45	1-4 1G RJ-45
Scale Numbers	AP: 1000 Stations: 5000 Spectrum Sensors: 100	AP: 15000 Stations: 75000 Spectrum Sensors: 750

Downloading the Virtual Machine Package File

You can download the virtual controller packages from the Fortinet Customer Support website. To access the support website you need a Fortinet Customer Support account. – **[URL required]**
The file name is, forti-wlm-x.x-xbuild-y-FWM-VM.ova, where x.x-x is the release version number. For example, 8.3.2.

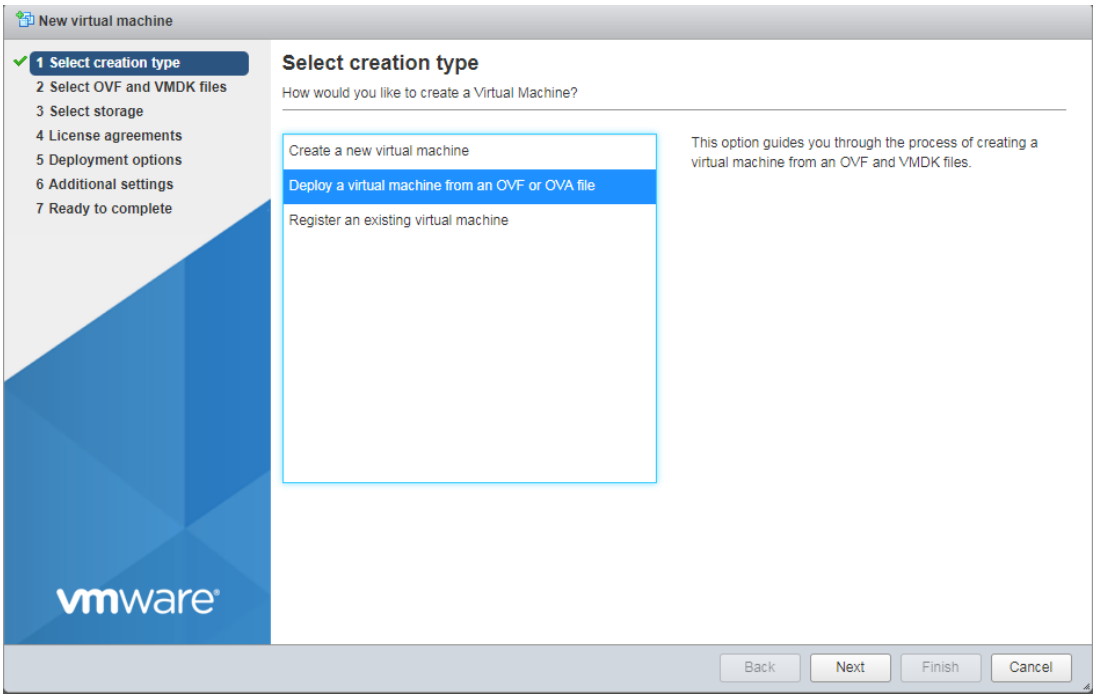
Creating the Virtual Machine

1. Open the VMWare ESXi console and navigate to **Virtual Machines < Create/Register VM**.

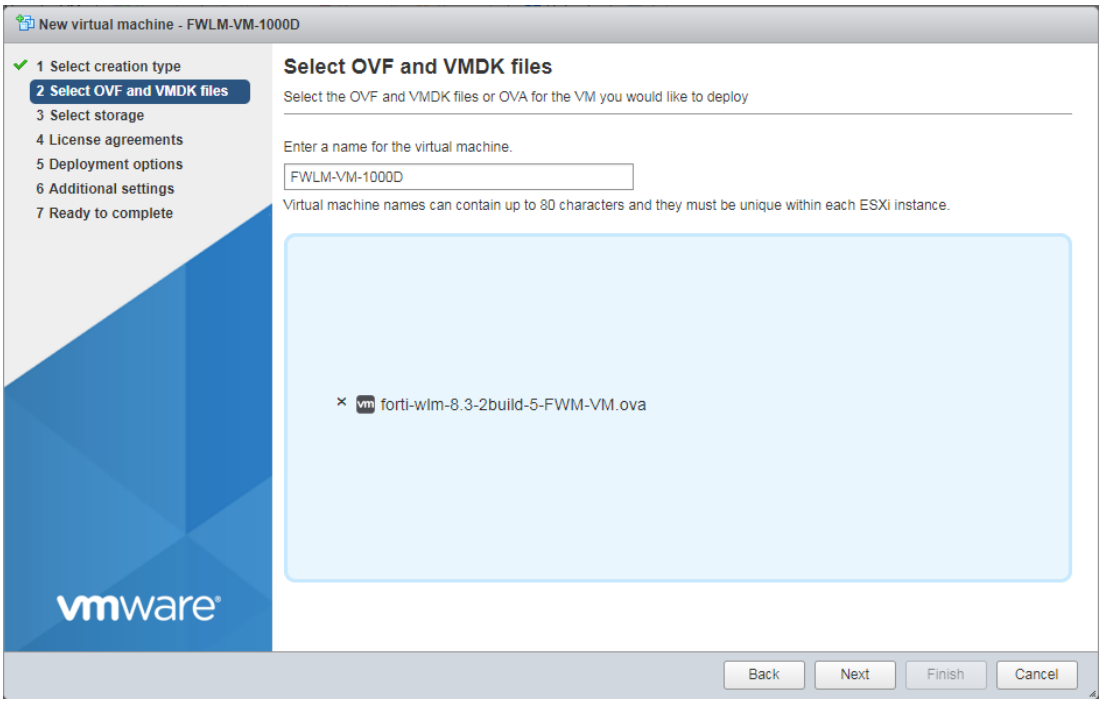


The **New Virtual Machine** wizard is displayed.

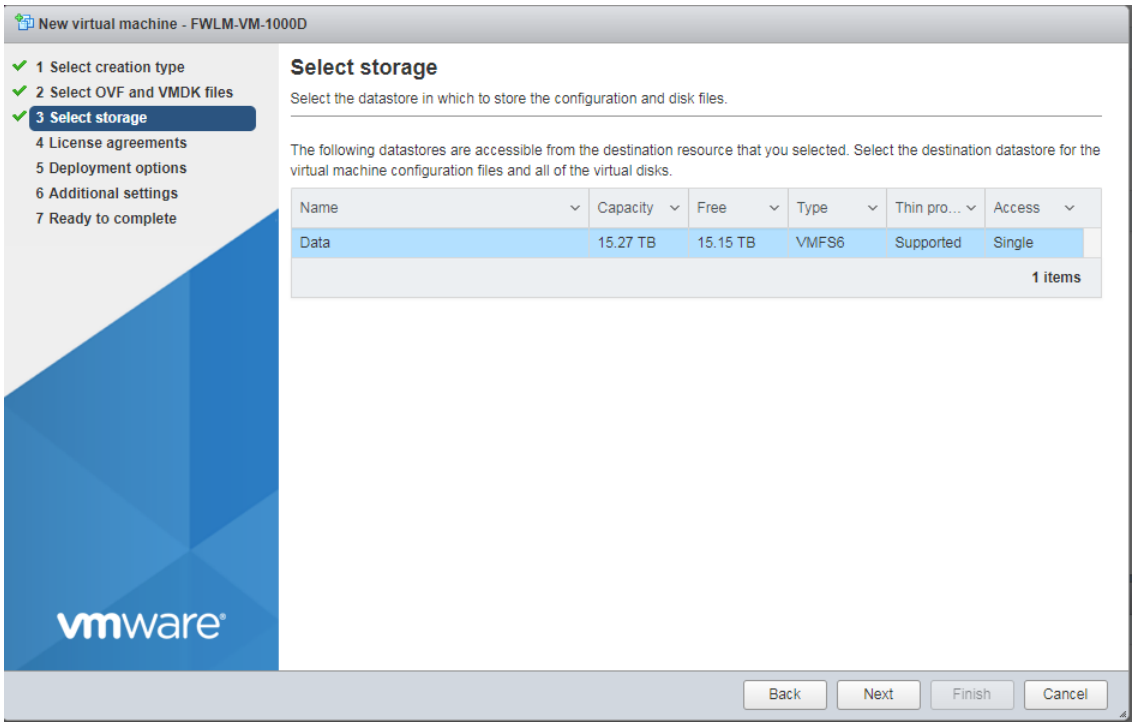
2. Select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.



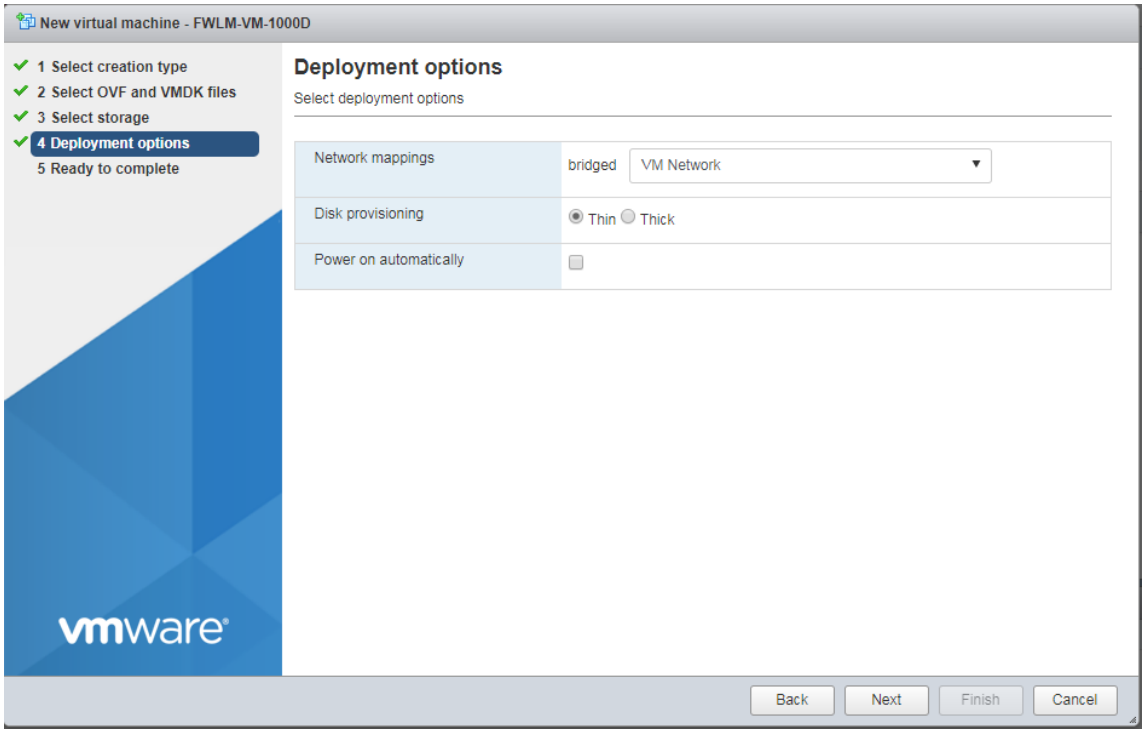
3. Enter a unique name for the virtual machine and click on the space, as indicated, to select or drag and drop the downloaded OVA file. Click **Next**.



4. Select the datastore to store configuration and disk files. Click **Next**.

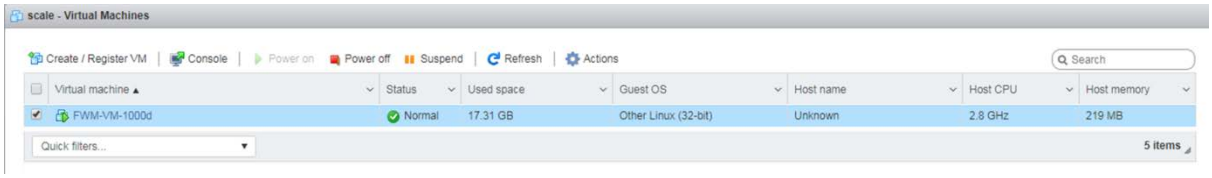


5. The deployment options are displayed. Click **Next**.
6. Select the **Network mappings** as **bridged VM Network**, **Disk provisioning** should be **Thin**. Disable **Power on automatically**. Click **Next**.



7. Review the configured settings and click **Finish**.

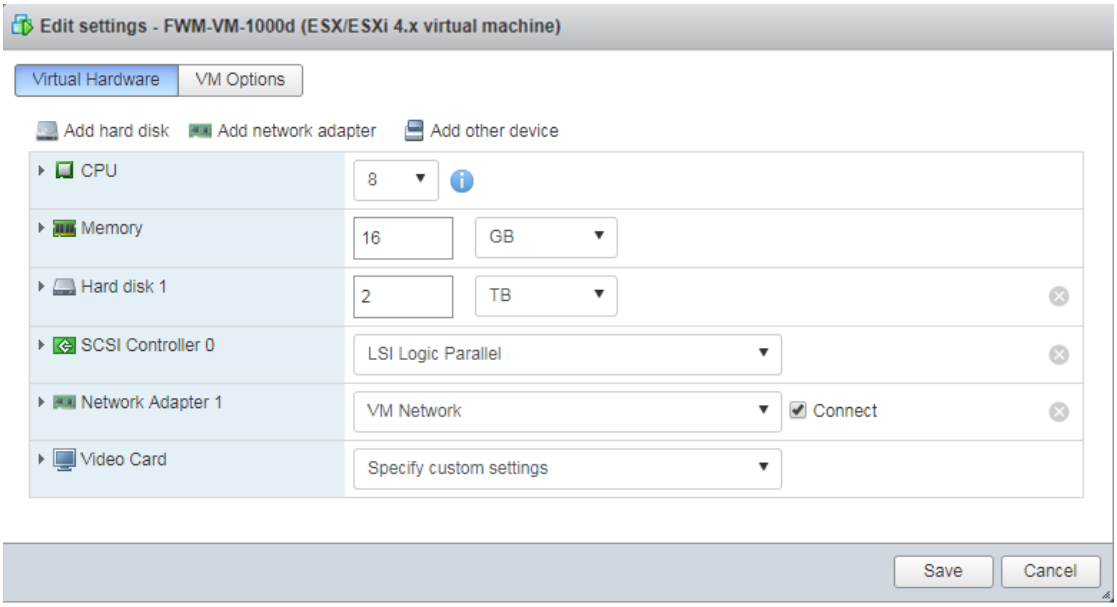
The virtual machine is created.



Configuring the Virtual Machine

After creating a virtual machine, configure it to work as a FWLM-VM-100D or FWLM-VM-1000D. See section Supported Hardware Configuration.

1. Select the listed virtual machine and right-click. Select **Edit settings**.
2. Modify the **CPU** and the **Memory**. Click **Add hard disk** to add a new hard disk. Click **Save**.



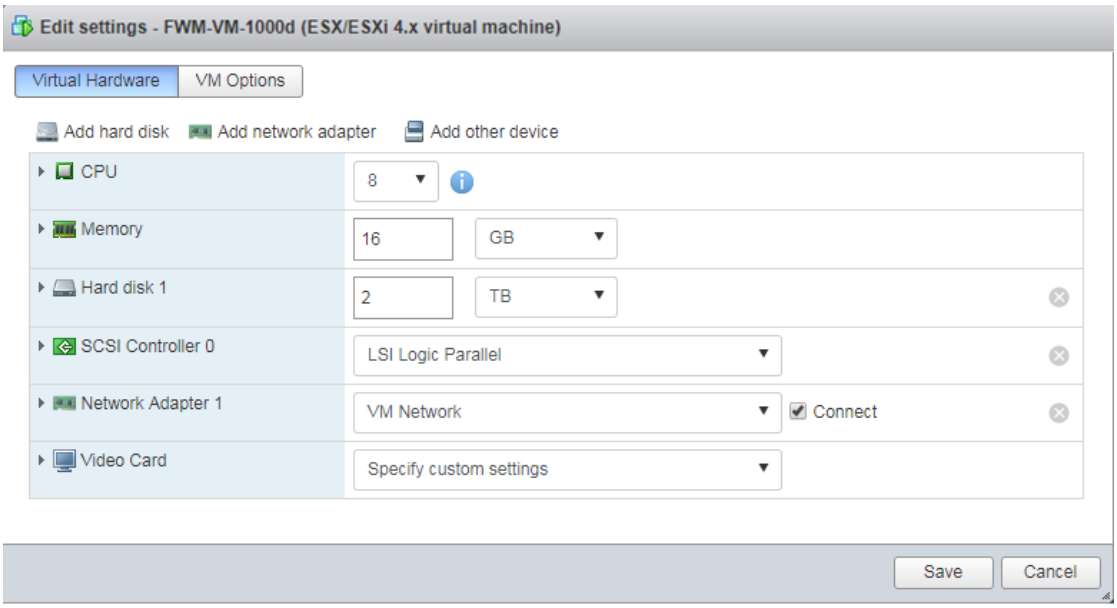
Starting the Virtual Machine

After configuring the newly created virtual machine, select the listed virtual machine and right-click. Select **Power < Power on**.
The Virtual Machine starts.

Expanding the Virtual Hard Disk

You can increase the storage space of a virtual machine by expanding its virtual hard disk. Follow these steps to expand the virtual hard disk.
Note: Decreasing the size of the virtual hard disk is not supported.

1. Run the **resizedisk** command from the IOS CLI to enable resizing the disk.
2. Select the virtual machine on the ESXi console and right click.
3. Select **Power < Power off** to power off the Guest VM.
4. Right click the virtual machine and select **Edit Settings.**
5. Under **Virtual Hardware,** modify the hard disk size (Supported Hardware Configuration)**.**



6. Click **Save.**
7. Right click and select **Power < Power on** to power on the Guest VM.

New Features

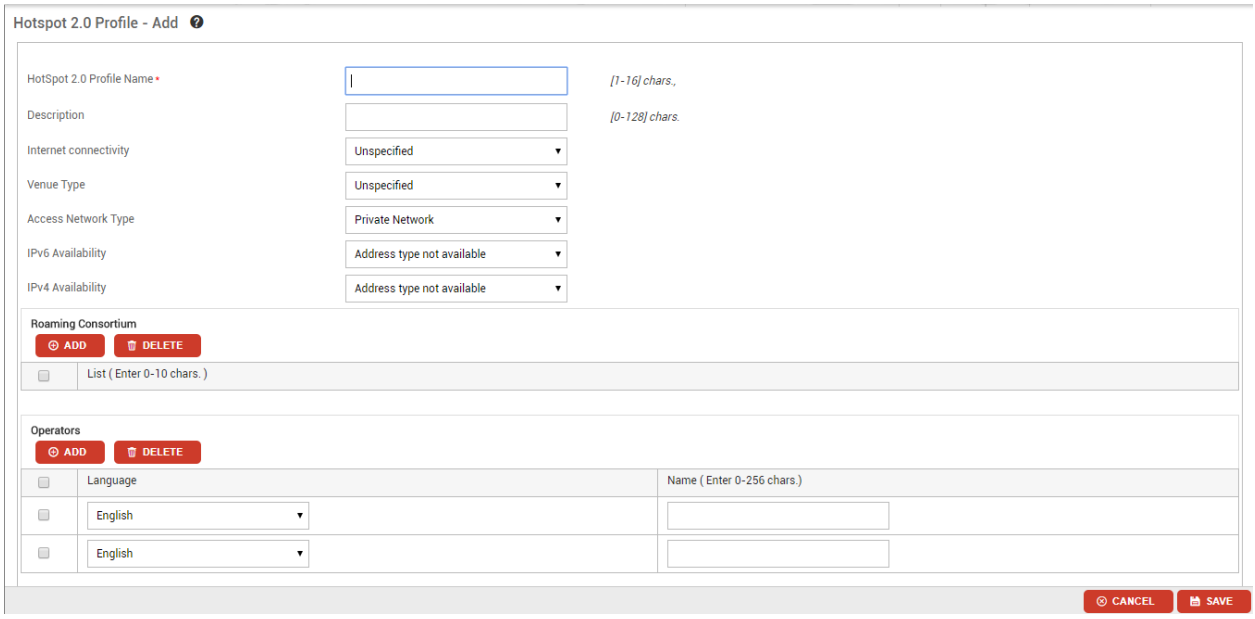
- Hotspot 2.0 Enhancements
- Spectrum analysis support in FAP
- Beacon Services Enhancements
- Controller Inventory Enhancements

Hotspot 2.0 Enhancements

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between WiFi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.
The Hotspot Profiles can be created from the **Configuration > Profiles > Hotspot 2.0** page. By default, the page shows the following details about a Hotspot Profile.

Add Hotspot 2.0 Profile

To add the Hotspot 2.0 profile, click the ADD button. In the pop-up box, enter a name for the Hotspot 2.0 Profile Name.



Update the following configuration.

Field	Description
HotSpot 2.0 Profile Name*	The name of the Hotspot 2.0 profile
Description	Description about the Hotspot profile
Internet connectivity	Range: On/Unspecified Default: Unspecified

	Specifies if connectivity to Internet is allowed
Venue Type	The venue type field in the information element provides additional information about the group and type of hotspot venue. The hotspot operator shall configure the Passpoint AP with one of the venue group description values, such as "business" or "educational" from the drop down box.
Access Network Type	The access network type field is automatically included in the IEEE 802.11u interworking element present in beacon and probe response frames in PAPs. Mobile devices can use this information when selecting a hotspot. The access network types are as follows: • Private Network • Private Network with Guess Access • Chargeable Public Network • Free Public Network • Personal Device Network • Emergency Services Only Network • Test or Experimental Network • Wildcard Network
IPv6 Availability	Select the IPv6 availability from the drop-down list. The default selection is Address type not available, and the options are as follows: • Address type available • Address type not available • Availability of the Address type not known
IPv4 Availability	Select the IPv4 availability from the drop-down list. The default selection is Address type not available, and the options are as follows: • Address type available • Address type not available • Availability of the Address type not known • Port-restricted IPv4 address available • Single NATed private IPv4 address available • Double NATed private IPv4 address available • Port-restricted IPv4 address and single NATed IPv4 address available • Port-restricted IPv4 address and double NATed IPv4 address available

Roaming Consortium	Enter the roaming ORG ID for the Hotspot profile. The valid range is 0-10 characters.
Operators	Select the Language from drop down list and enter the Operator Name in the range 0-256 chars.
Venue	Select the Language from drop down list and enter the Operator Name in the range 0-256 chars.
3GPP Cell Network	• Enter Country Code. • Enter the 3GPP cell network MCC; the default value displayed is 0, and the valid range is 0-999. • Enter the 3GPP cell network MNC; the default value displayed is 0, and the valid range is 0-999.
Domain	Enter the domain name for the Hotspot profile. The valid range is 0-128 characters.
NAI	NIA Realm: Enter the NAI realm. Realms that can authenticate a mobile device's username/password or certificate credential shall be added to this list. The valid range is 0-50 characters. Realm Auth Method: Select the NAI realm authentication method from the drop-down list. The default selection is EAP TLS Certificate and the options are as follows: • EAP TLS Certificate • EAP TLS MSCHAPv2 Username/Password • EAP SIM • EAP AKA • EAP AKA`
ADVANCED SETTINGS	Advance Settings supports following : WAN Metrics: Connection Capability: Connection capabilities allow the user to allow/block protocols. There are a set of system defined protocols as listed above. In addition, the user can also create rules for custom protocols Qos Map: Once the profile is created, additional parameters are available under Advanced Settings,

	OSU Settings: There are additional OSU Provider Settings: Friendly Names Icons Methods Description

Spectrum analysis support on FAP

This release of FortiWLM introduces Spectrum Analysis support for FAP-U421EV and FAP-U423EV Access Points with Advanced Interference detection mechanism added.

Users can deploy these Access Points (Sensors) in their Wireless network which will scan the environment continuously for Interference and send reports to Spectrum Manager on the Interference detected.

Users are allowed to configure both radios of these sensors in **Scan Spectrum** Mode, which will make the radios to scan the Spectrum.

Supported APs

- FAP-U421EV
- FAP-U423EV

Spectrum Sensors detects the following non-802.11 interference devices

- Microwave Oven (conventional)
- Analog Cordless Phone (2.4 and 5 GHz)
- Wireless video camera (2.4 and 5 GHz)
- Wideband RF Jammer
- Narrowband RF Jammer
- S-Band radar-based motion detector
- DSSS Cordless Phone (2.4 and 5 GHz)
- Digital Baby Monitor – Single Carrier
- Microwave Oven (inverter)
- Xbox wireless game controller
- Bluetooth Device
- FHSS Cordless Phone (2.4 and 5 GHz)
- Possible Interferer

Enabling Spectrum Analysis

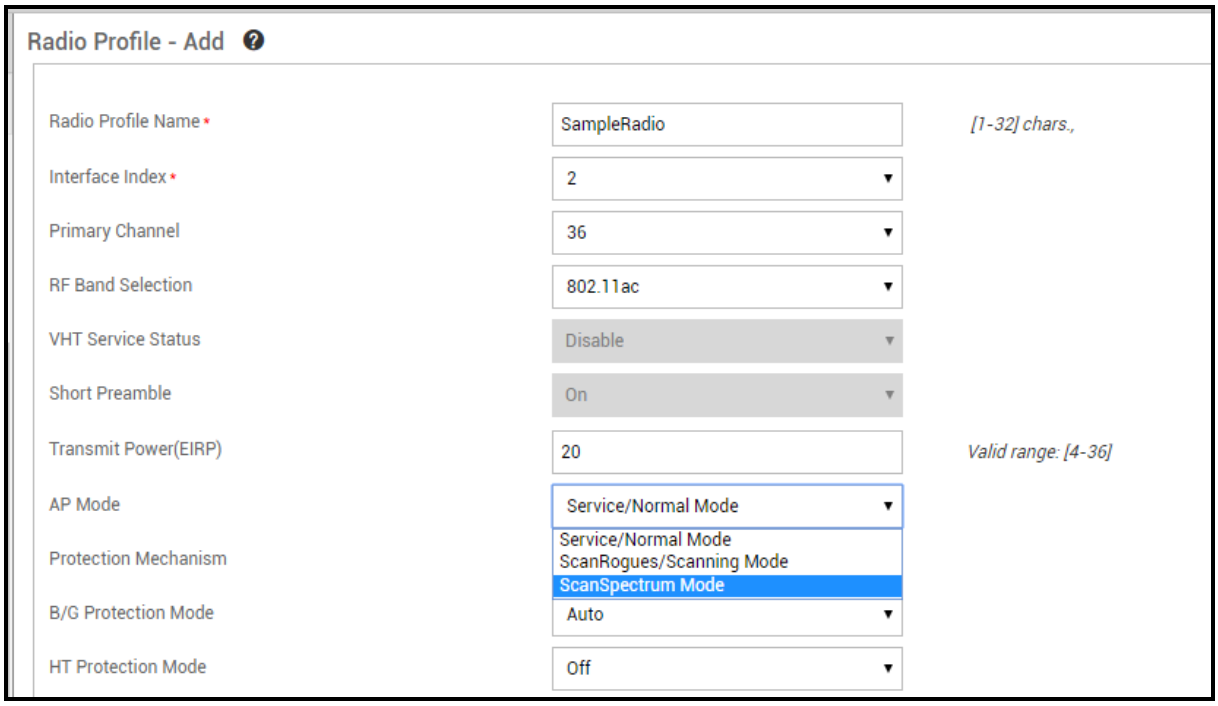
Access Point radios can be configured **Scan Spectrum Mode** using following ways:

Configure Scan Spectrum Mode for Sensor from FortiWLC-SD

1. Navigate to Configuration > Wireless > Radios.
2. Click the "***Edit***" icon of the respective radio for the need to be enabled to scan spectrum.
3. Change the "**AP Mode**" from "***Service Mode***" to "***Scan Spectrum Mode***" mode.

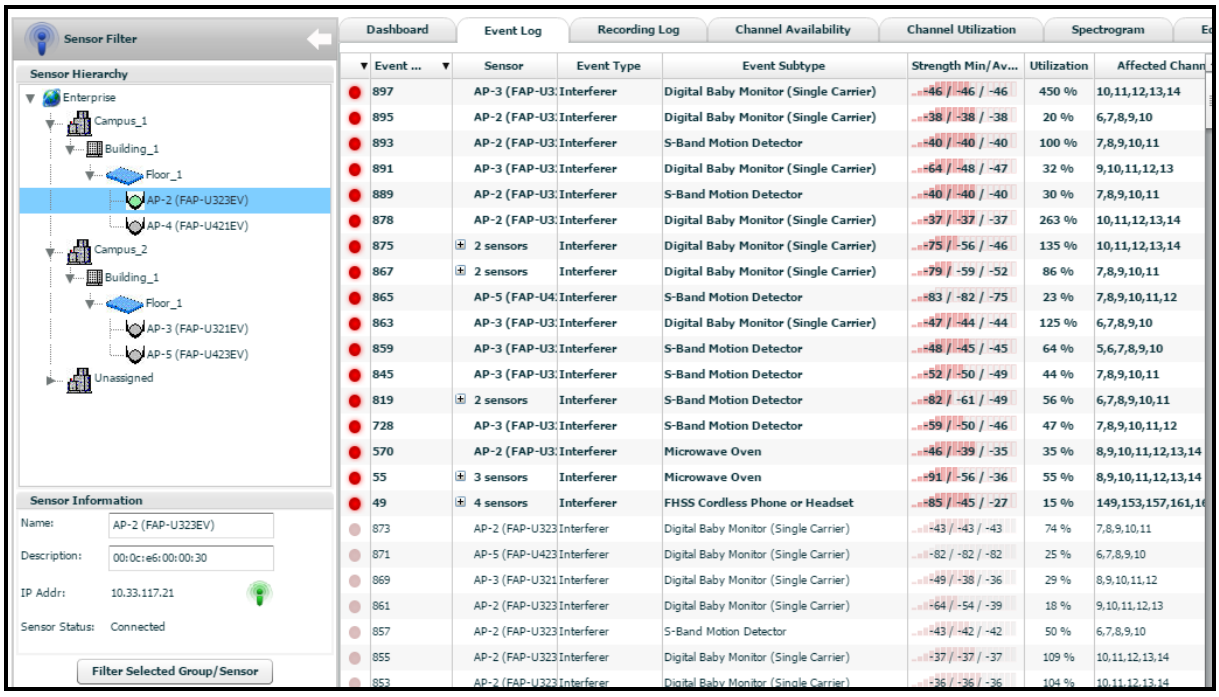
Configure Scan Spectrum Mode for Sensor from FortiWLM

1. Add **Radio Profiles** with **AP Mode** as "***ScanSpectrum Mode"***



2. **Create** an **AP Group** with Sensors added into group.
3. **Add** an **AP Template** and **Register** to the AP Group.

Once **Scan Spectrum** is enabled for a particular radio of sensor, sensor starts scanning and reports ***events*** to Spectrum Manager.



Note:

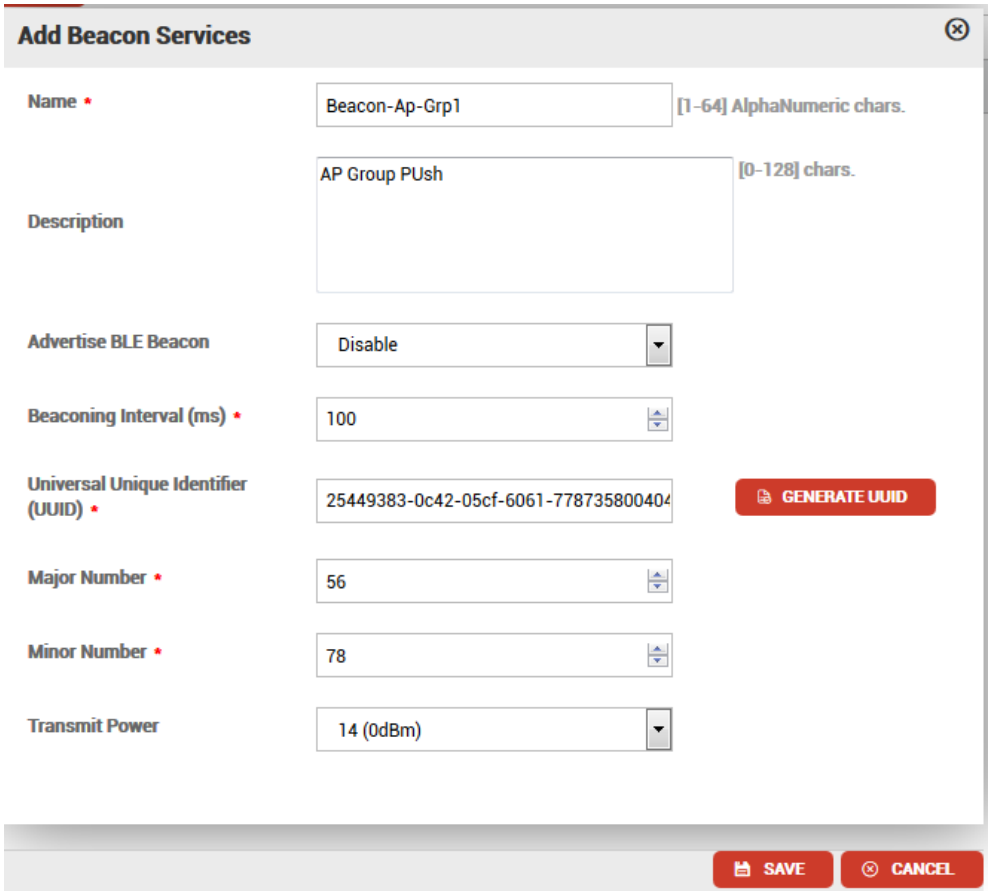
- Each radio interface of the AP scans only the corresponding band (2.4GHz or 5GHz) it is configured for.
- The APs need to be discovered in L3 mode for the scan spectrum functionality to work.
- The AP will not service clients in '**Scan Spectrum mode'**

Beacon Services Enhancements

With this release of FortiWLM, User will be able to push Beacon Services and can map the AP's with specific Service.

Supported APs:
Wave1 AP's: AP122, AP822, AP832 (these APs will require a Bluetooth dongle)
Wave2 AP's: FAP-U421EV and FAP-U423EV (these APs have inbuilt hardware)

To use the beacon services, navigate to **Configuration > Controller Configuration > Beacon Services** and click the **ADD** button to enter the following details:

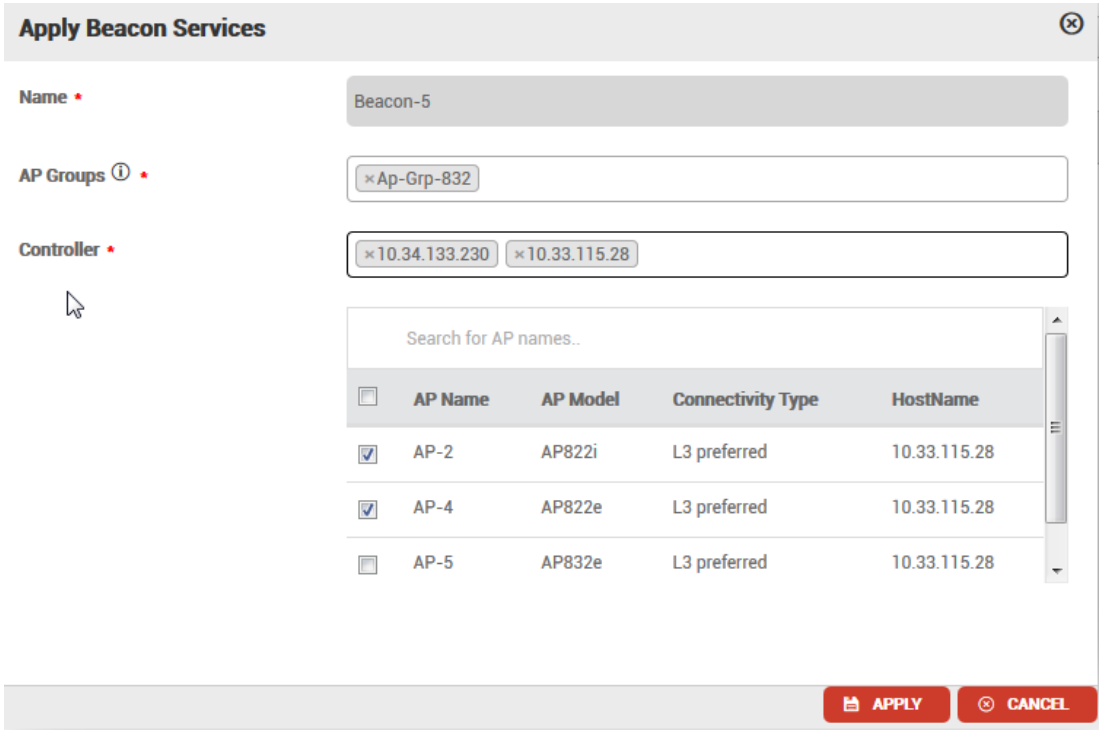


- Enter a **Name** for the Beacon Services and provide a **Description**.
- Enable **Advertise BLE Beacon** to start the service.
- Select the **Beaconing Interval** at which the beacons are sent.
- Enter a **Universal Unique Identifier (UUID)** that is specific to your network and also specify the respective **Major Number and Minor Number**.
- Select **Transmit Power**.

After creating a profile, click the action arrow to push this to push them to APs or AP Groups via FortiWLM.

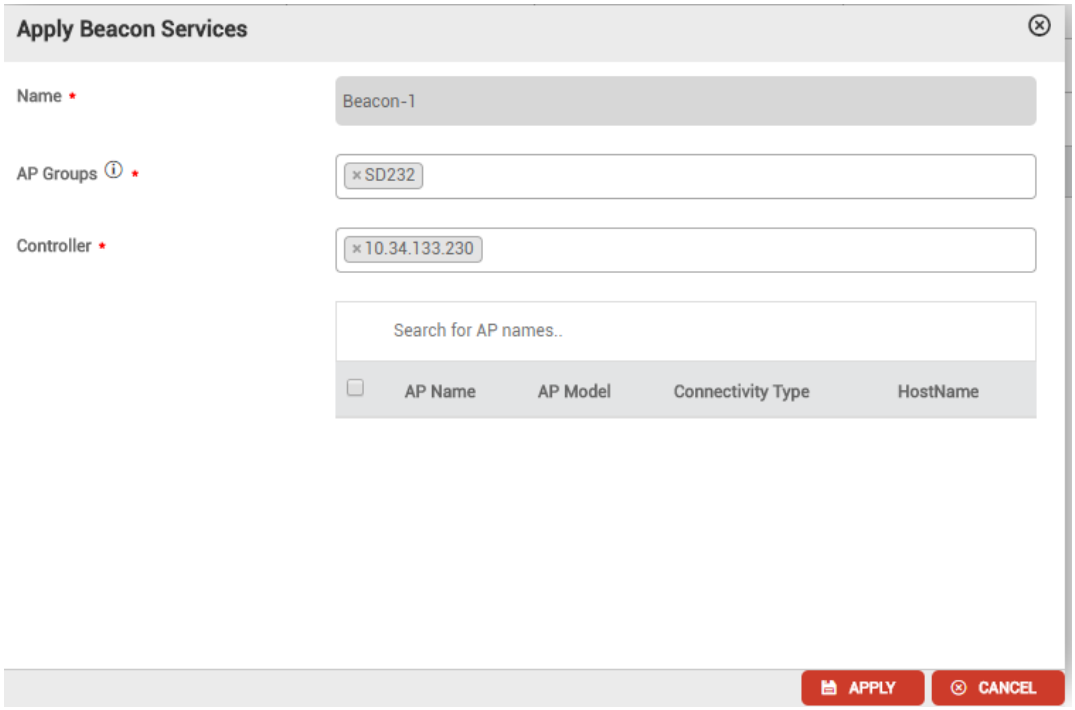
To push the profile to Controllers

Click on **APs on Controller** select the available and supported version controllers are 8.3.0, 8.3.1 and 8.3.2 controllers from the controllers drop-down. Select the list of APs and click on **APPLY**.



To push a specific profile to AP Groups

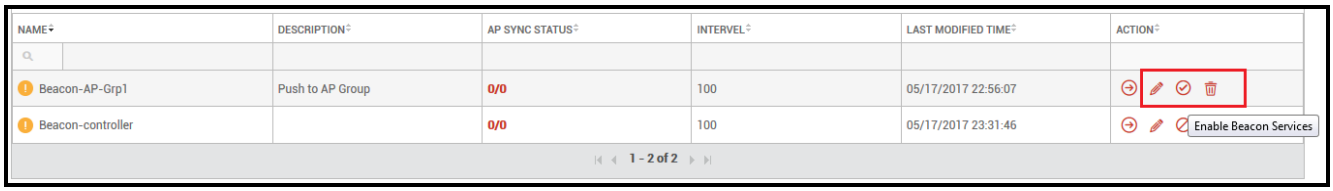
Select **All APs on AP Group** and select AP groups from the AP Group drop-down and click on **APPLY** button.



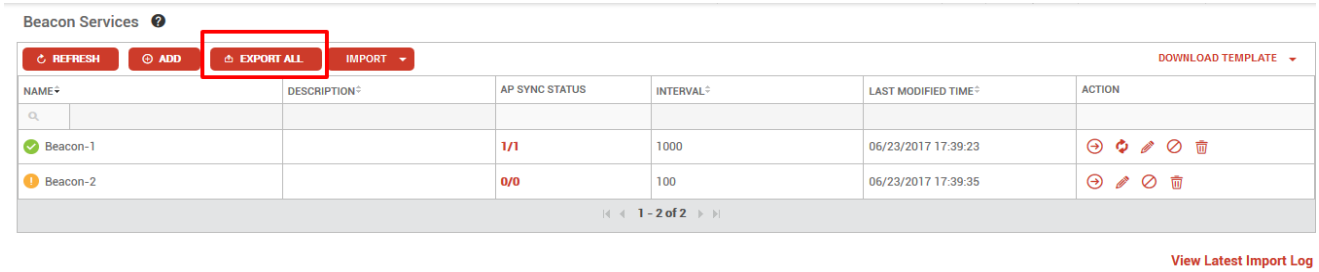
You can edit a Beacon Service; click the edit icon in the **Action** column.

Similarly, you can Delete, Enable/Disable a beacon Service clicking respective icon on the action column.

Note: After upgrading FortiWLM to 8.3.2, the existing Beacon profiles need to be re-applied to the APs.



Alternatively, you can load Beacon Services profiles by importing files (*.csv). Click the **IMPORT** button and export the existing beacon profiles by clicking on **Export All** button.
Note: The **Export All** option exports the Beacon profile, but does not export the associated APs.

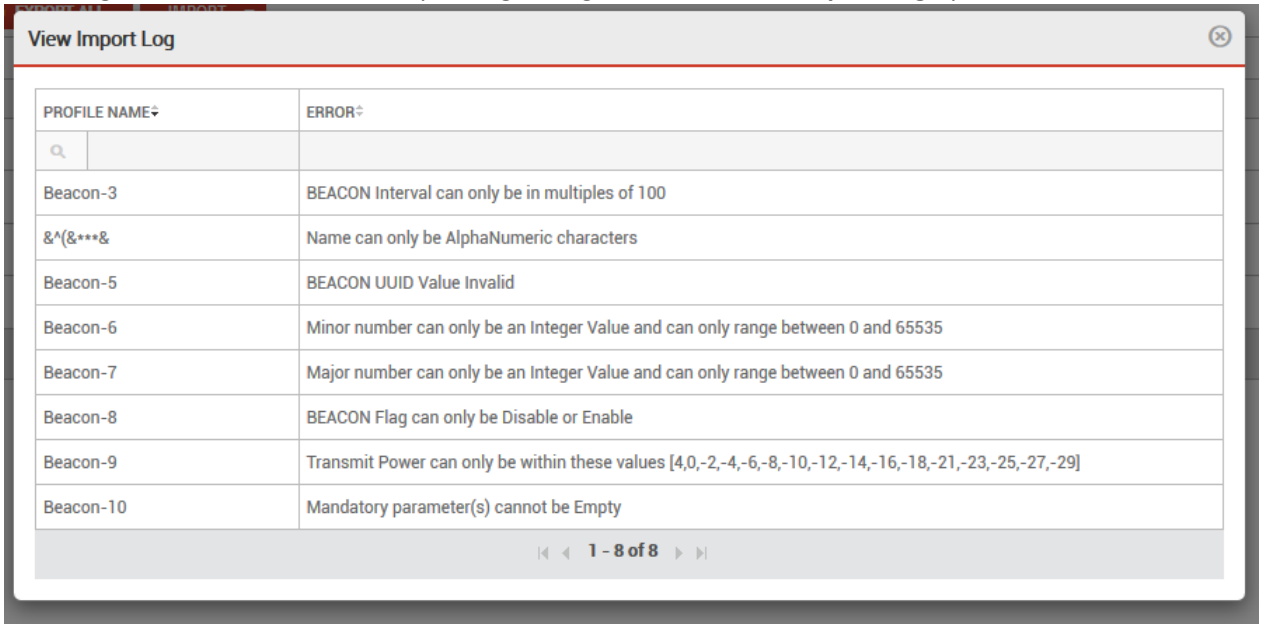


You can download the default profile and deployment templates using the **Download Template** option.

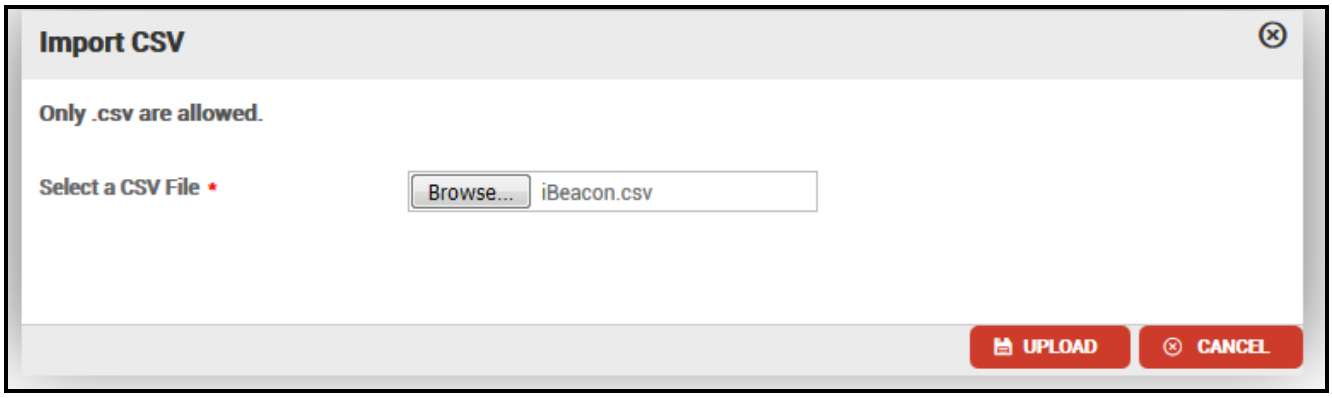
	A	B	C	D	E	F	G	H
1	name	uniqueidentifier	interval	minornumber	majornumber	descr	blebeacon	transmitpower
2	Beacon-3	545f4426-2896-0785-2c75-97d178e2a613	400	45	56		Enable	-18

	A	B	C
1	name	controllerId	apId
2	Beacon-2	4	1:2:3

Edit these templates and upload import them into the WLM using the **Import** option and register them. If the registration fails, view the import logs using the **View Latest Import Log** option for failure details.



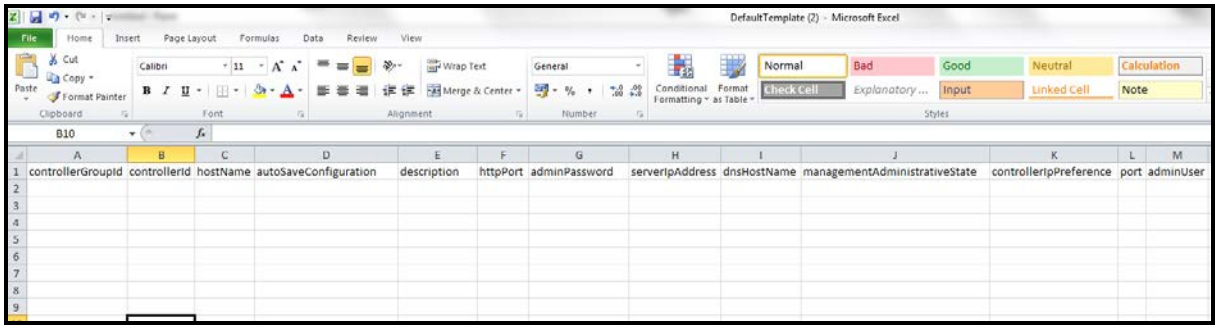
Browse the *.csv file you want to load and click on upload.



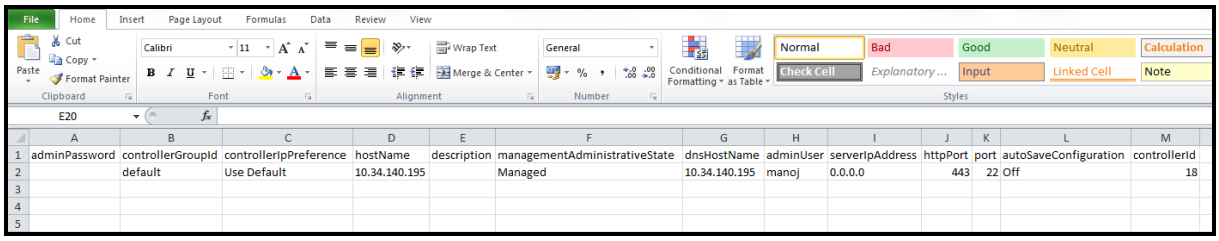
Controller Inventory Enhancements

You can add multiple controller entries in Inventory page using IMPORT functionality.

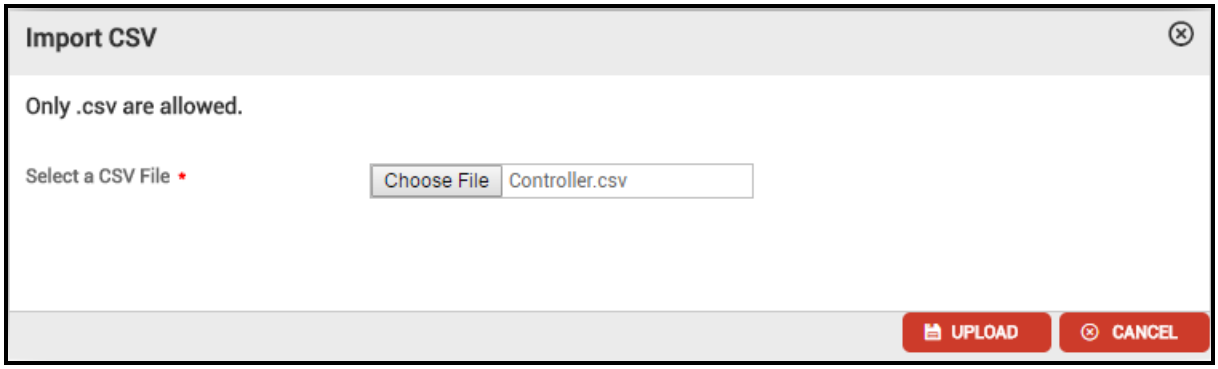
1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers** page will be displayed.
3. Click on **DOWNLOAD DEFAULT TEMPLATE** or **EXPORT ALL** button.
4. Download the controller.csv file
5. Open the controller.csv file



6. Enter the values for controller entry and save it.



7. Click on **IMPORT** and select the controller.csv file.

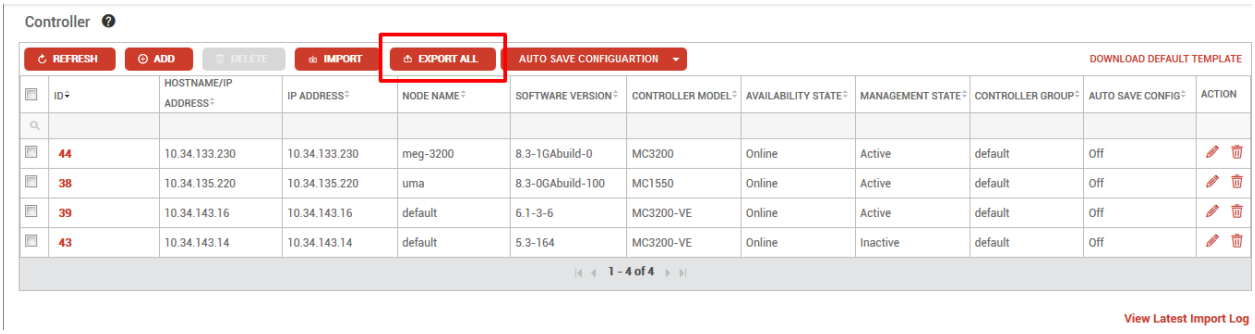


8. Click on UPLOAD and controller entry gets added in the Inventory page.

Export Functionality

You can export multiple controller entries to update existing entries using the export functionality.

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers** page will be displayed.
3. Click on **EXPORT ALL** button.



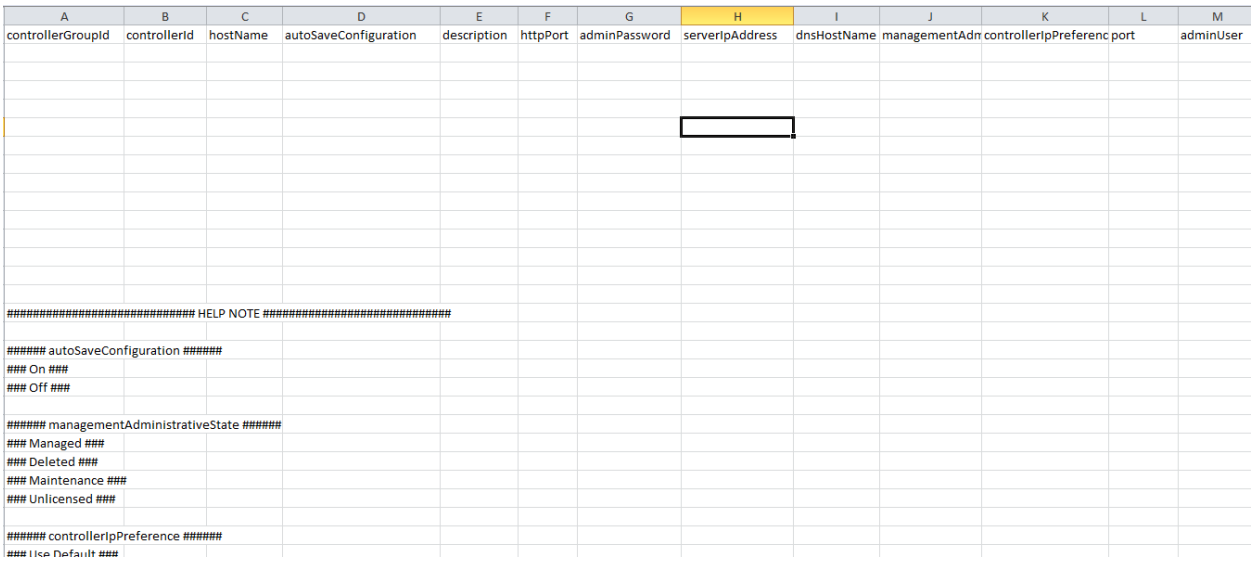
4. Controller.csv will download on your local drive.
5. Controller entries will display in controller csv file.

NOTE: The Controller password will not download from export functionality

Default Template

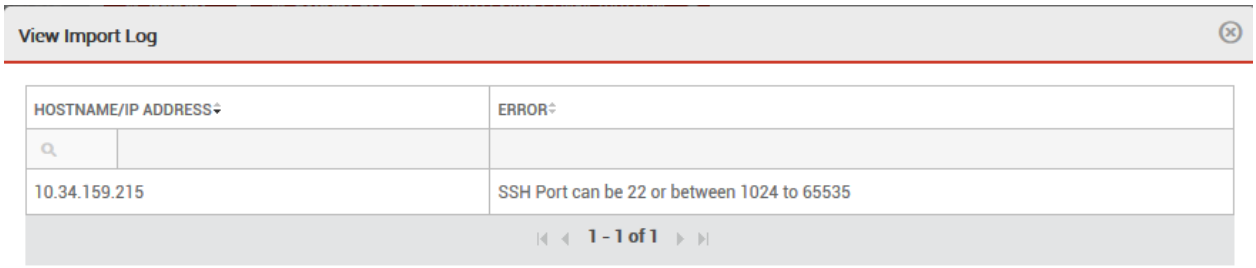
The default template is used as reference template for adding multiple controller entries in the controller.csv file.

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers** page will be displayed.
3. Click on **DOWNLOAD DEFAULT TEMPLATE**.



4. Controller.csv file downloaded in local drive.
5. Open the file and enter the controller entries.
6. Save the controller.csv file and import the file in Inventory page using IMPORT option.

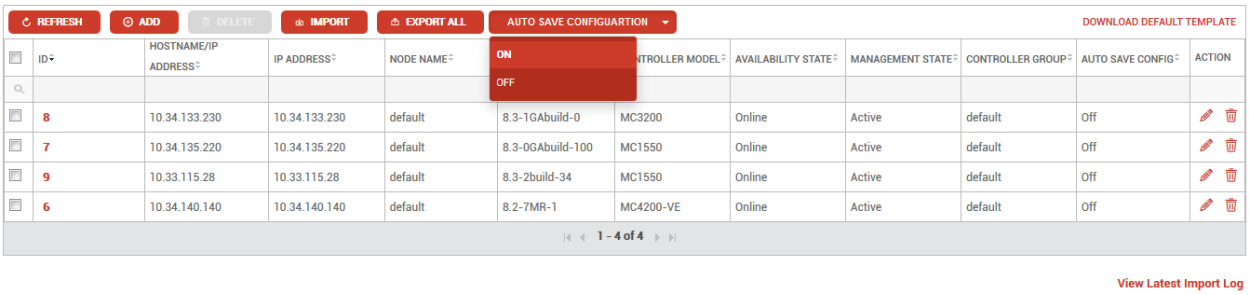
If the import fails, click **View Latest Import Logs** to see the import logs for failure details.



Auto Save Configuration

Auto Save Configuration ON/OFF option is used to apply on multiple/bulk controllers entries in inventory page.

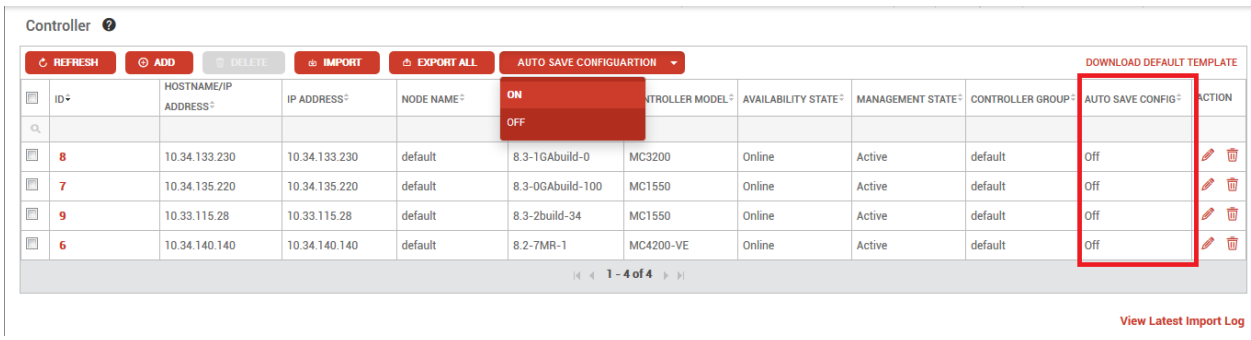
1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and Controllers page will be displayed.
3. Select the controller entry.
4. Select ON from the **Auto Save Configuration** drop down.
5. AUTO SAVE CONFIG column is updated for the controller entry.



6. Once again select the controller entry.
7. Click on Auto Save Configuration > OFF.
8. **AUTO SAVE CONFIG** column is updated for controller entry.

Auto Save Config column added in Inventory Page

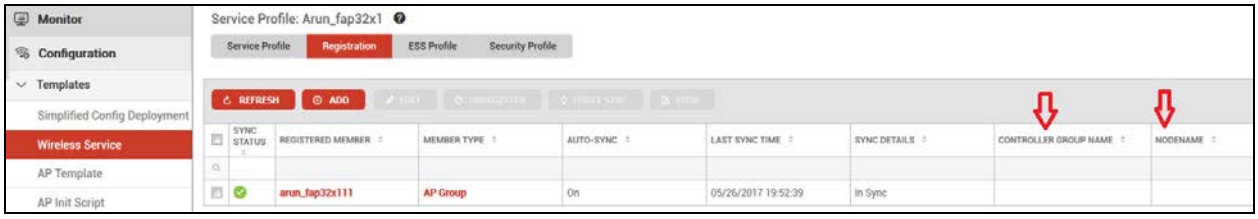
1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controller** page will be displayed.
3. Add one controller
4. Auto save config column will display in controller entry.



Controller Group Name and Node Name columns added in Service Profile Registration Page

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers**, Add Controller page will be displayed.

3. Add Controller.
4. Go to Templates.
5. Click on Wireless Service profile.
6. Create a profile and register to the controller.
7. CONTROLLER GROUP NAME and NODENAME column added in Service Profile Registration Page.



Known Issues and Limitations

Bug ID	Summary	Workaround
423760	FWLCVM: Controller discovery in FortiWLM is failing on n+1 failover with auto revert disabled	
414104	Spectrumd crashing continuously when both the Radios of FAP42X have enabled Scan Spectrum Mode	
420172	AIRIQ: Axis Parameters are not displayed in FFT data charts for 2.4GHz Channels	
437402	SAM: Baseline tests are failing for AP1020 and AP832 for RADIUS and WPA2PSK profiles	Use clear profiles for Baseline tests
438002	ARRP profiles are not getting to group level APs	Edit the synced profile, which would re-sync the updated profile to AP
433862	After pushing the ARRP profile to an AP from the FortiWLM, the configurations are not pushed to that AP	Push other profiles related to AP before pushing the ARRP profile
423984	Mismatched APs are reported even if the Controller and FortiWLM have same values	
438751	The VRRP IP interface does not get the IP address assigned.	

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service